Bastille

A Walk Through Your Airspace: Understanding the IoT from DC to 10GhZ

HITB GSEC SINGPAORE, October 14, 2015

Presenter:

Chris Rouland

Founder, Chairman and CTO

@chris_rouland

- **Founder and CEO, Endgame Systems**
- **CTO, Internet Security Systems**
- **Director of X-Force, Internet Security Systems**

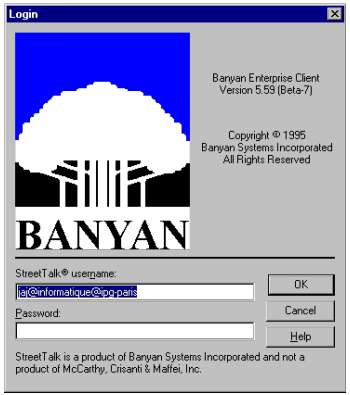

Bastille
THE PROBLEM
By 2020
50 BILLION DEVICES
NO SECURITY

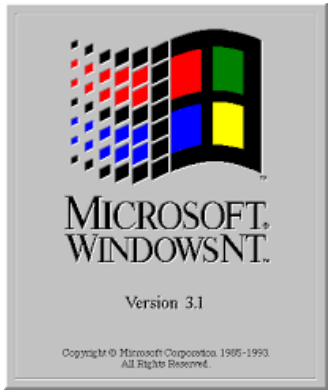
THE EARLY DAYS

The rise of early hackers, past and present

EARLY DAYS

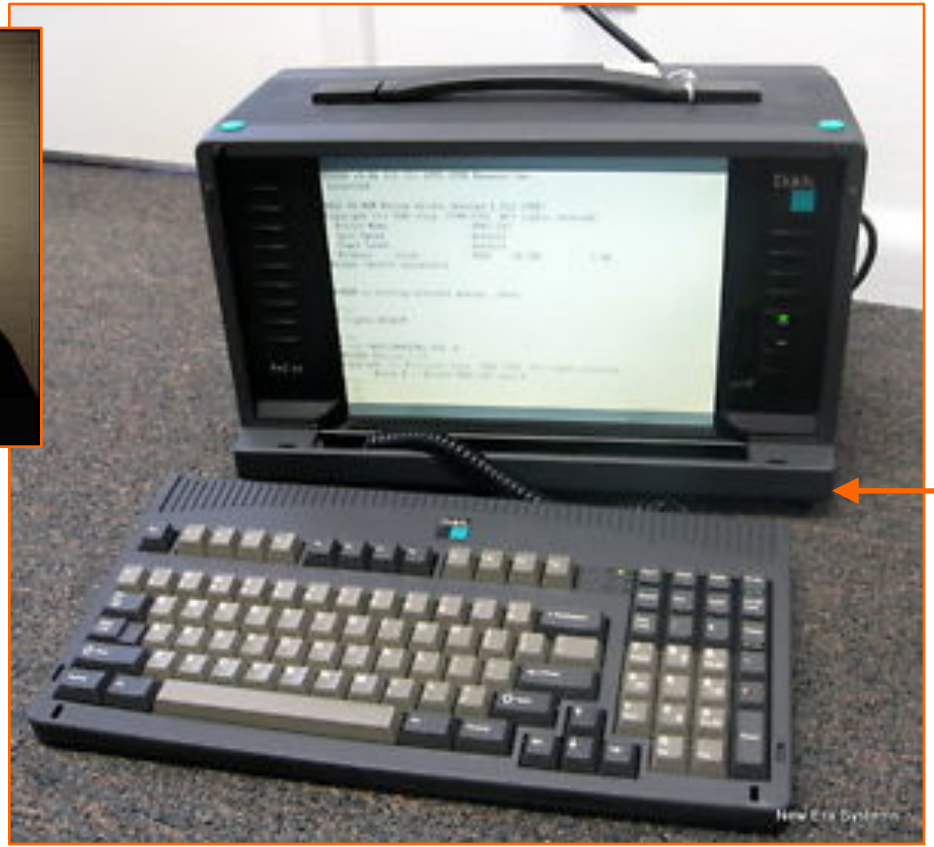
Finding Our Way





Bastille

Chris Rouland
Bastille
Founder/Chairman/CTO



Network General
Packet Sniffer
($25k)

Wireless Threat surface expanding way beyond Wired surface

2014: Mobile usage officially overtakes PC usage

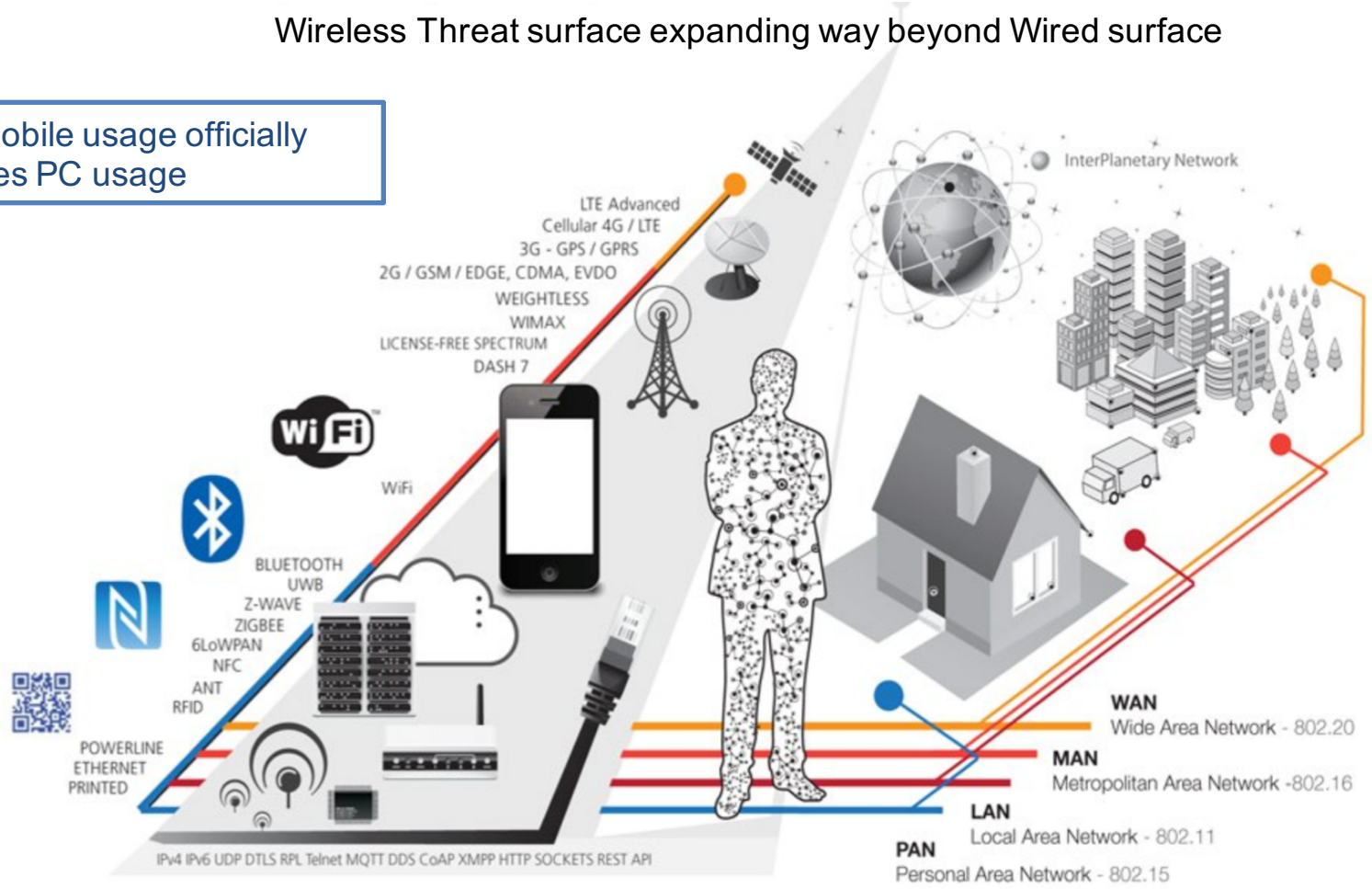
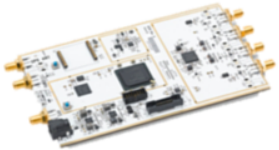


Photo: Postscapes

INNOVATION

Still a mess

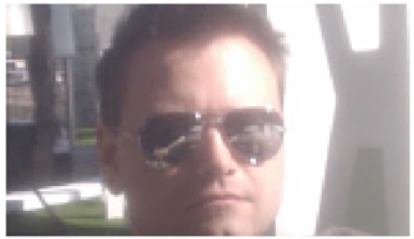
Bastille

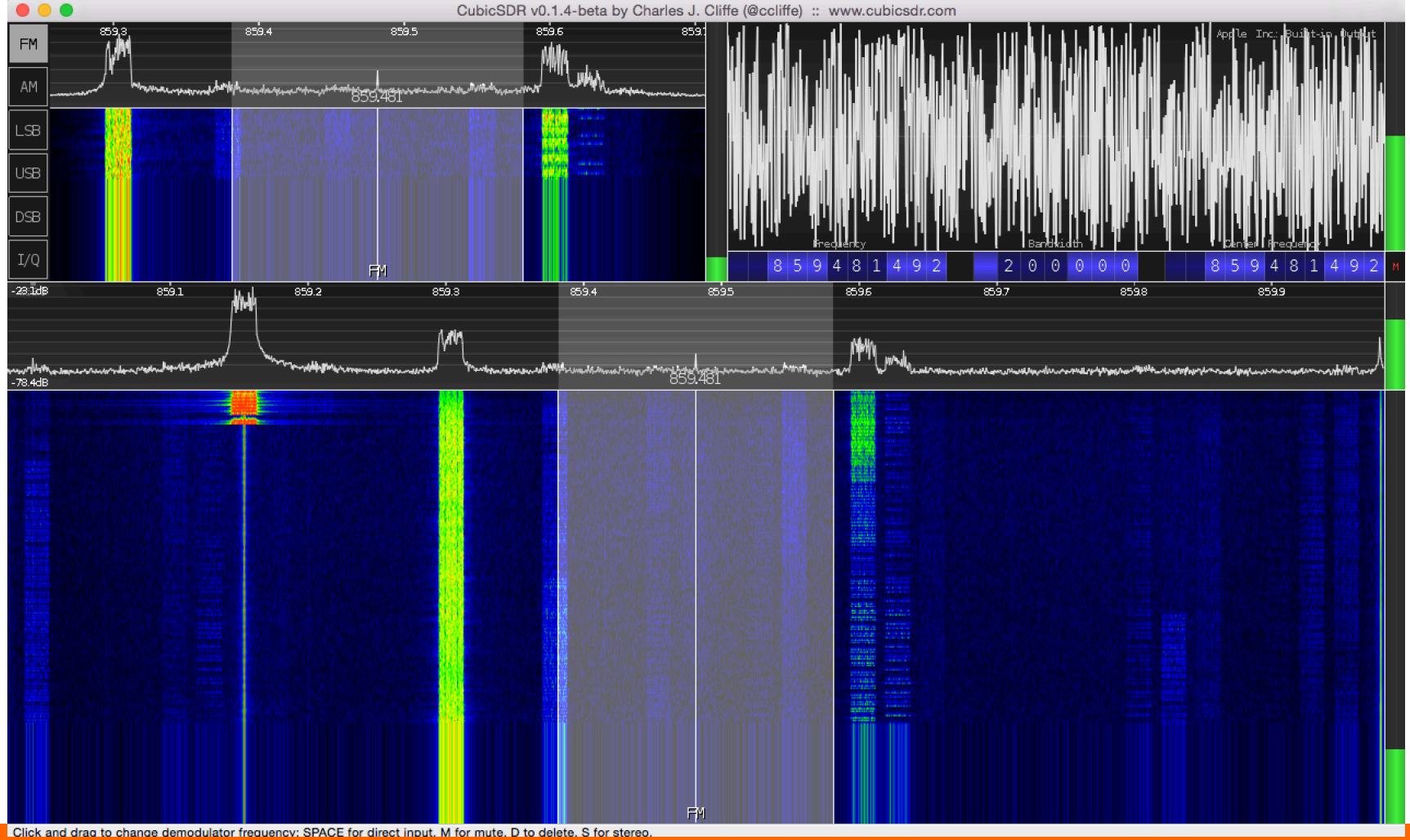


IoT and Software Defined Radio

$20 - $1000

60 MHz to 6 GHz

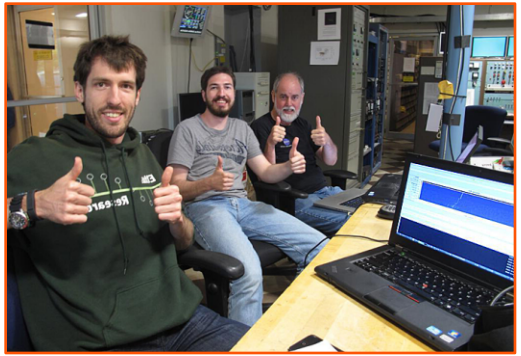


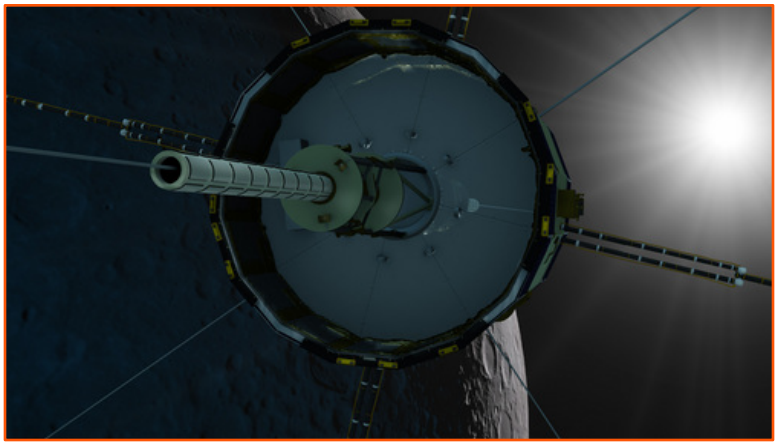

CubicSDR v0.1.4-beta by Charles J. Cliffe (@ccliffe) :: www.cubicsdr.com
FM
AM
LSB
USB
DSB
I/Q
859.3
859.4
859.5
859.6
859.481
FM
Apple Inc.: Built-in Output
Frequency
Bandwidth
Center Frequency
8 5 9 4 8 1 4 9 2
2 0 0 0 0 0
8 5 9 4 8 1 4 9 2
-28.1dB
-78.4dB
859.1
859.2
859.3
859.4
859.5
859.6
859.7
859.8
859.9
859.481
FM
Click and drag to change demodulator frequency; SPACE for direct input, M for mute, D to delete, S for stereo.

Bastille

Hacking Satellites (ISEE-3)

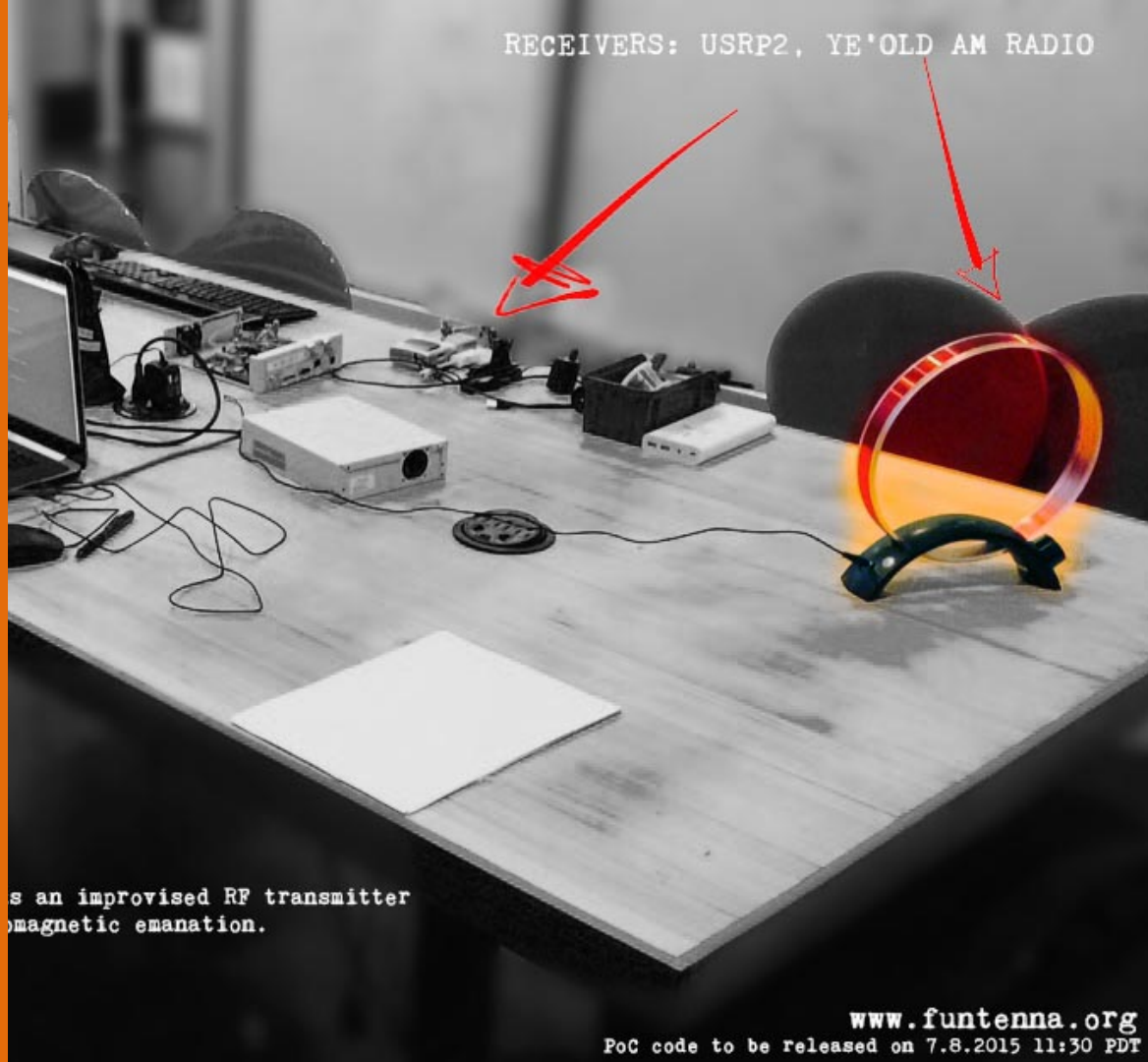
Balint Seeber
Bastille
Dir, Threat Research





FUNTENNA
radio based back channel

- Covert, wireless exfiltration
- Only needs a radio & firmware
- Completely invisible to existing network security
- New trend in data ex-fil



Hacking Cellular

Rogue wifi of 2010

- Showing up in the wild
- Cost went from 500k to $500
- World now depends on cellular 2-auth

ProxyHam

Anonymous Data Exfil

- Uses 900MHz as physical layer of obfuscation
- Allows hacker to proxy WiFi from up to 2mi away
- Addition of SIM card makes distance limitless

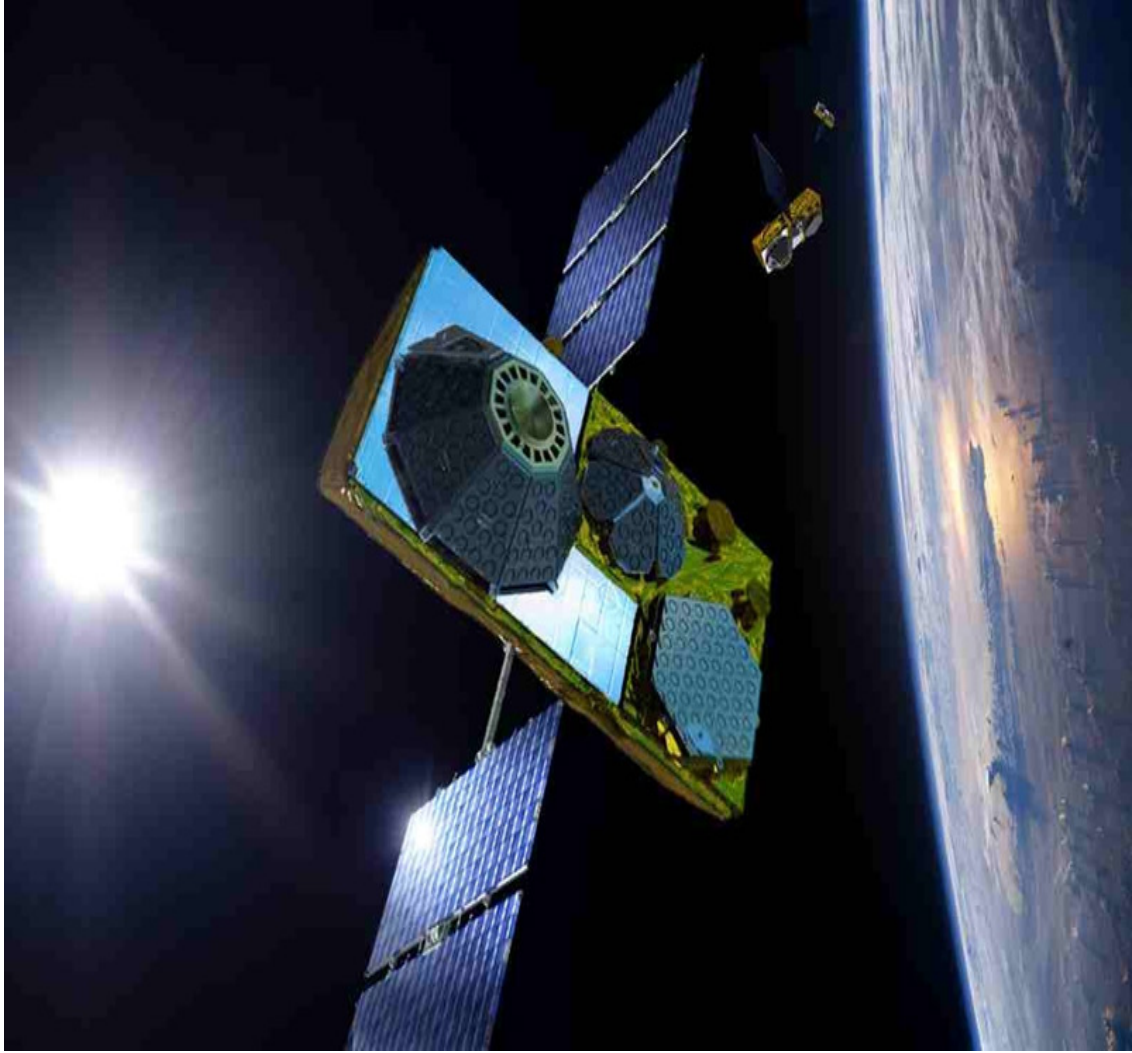
Samsung Fridge
Google Login Theft

- Connection to Google calendars
- No SSL cert validation
- Login details accessible to anyone that could access WiFi

Globalstar Network

Space is the new frontier

- Simplex Data Network
- Spoof and Jam
- HTTP not HTTPs



Ship Tracking Systems
Automated Identification System

- Fire man-overboard
- Override auto-pilot
- Insecure, running VHF

PCWorld

Researchers hack GSM mobile calls using $9 handsets *January, 2011*

WIRED

Researchers Hack Air-Gapped Computer With Simple Cell Phone *July, 2015*

engadget

Some SIM cards can be hacked in about 2 minutes with a pair of text messages *July, 2015*

NETWORKWORLD

Hackers show off long-distance Wi-Fi radio proxy at DEF CON *August, 2015*

WIRED

Big Vulnerability in Hotel Wi-Fi Router Puts Guests at Risk *March, 2015*

ars technica

Hacker Develops Device to Surf the Internet Anonymously *July, 2015*

ZDNet

Android smartwatches vulnerable to snooping
December, 2014

SANS

Bluetooth and its Inherent Security Issues
March, 2015

The Register®

Bluetooth privacy is mostly ignored, so you're beaming yourself to the world *July, 2014*

engadget

Researchers find major security flaw with ZigBee smart home devices *August, 2015*

GIZMODO

Philips Hue Light Bulbs Are Highly Hackable
August, 2013

NETWORKWORLD

Researchers exploit ZigBee security flaws that compromise security of smart homes *July, 2014*

The Register®

Simple 'open sesame' to unlock your HOME by radiowave *August, 2013*

Forbes

How Your Security System Could Be Hacked To Spy On You *July, 2014*

black hat®

Honey I'm Home - Hacking Z-Wave Home Automation Systems *November, 2013*

Crypto weakness in smart LED lightbulbs exposes Wi-Fi passwords *July, 2014*

'Bash' bug could let hackers attack through a light bulb *September, 2014*

Philips Hue susceptible to hack, vulnerable to blackouts *August, 2013*

CNBC

Biggest hacking threat to business? Wearables.
March, 2015

c|net

Fitness tracking goes under the security spotlight
July, 2014

WT VOX

Simple Hacking And Data Stealing In Wearables That Can Be Used Against You *September, 2014*

Forbes

How Hackers Could Use A Nest Thermostat As An Entry Point Into Your Home *March 2015*

COMPUTERWORLD

Black Hat: Nest thermostat turned into a smart spy in 15 seconds *August, 2014*

VentureBeat

I control your thermostat. Google's Nest gets hacked *August, 2014*

INTERNATIONAL BUSINESS TIMES

'Extremely chatty' Samsung smart TVs pose major security risk to government, healthcare and energy companies *March 2015*

black hat®

Hacking, Surveilling, and Deceiving Victims on Smart TV *August, 2014*

SC MAGAZINE
FOR IT SECURITY PROFESSIONALS

Alarm bells ring for Internet of Things after smart TV hack *June, 2014*

The New York Times

The August Smart Lock Shows Why You Should Stick With Dumb Keys *October 2014*

WIRED

Millions of Kwikset Smartkey Locks Vulnerable to Hacking *August, 2013*

tom's GUIDE

This 'Smart' Lock May Have Dangerously Dumb Security *March, 2015*

InformationWeek DARKReading

Five Ways To (Physically) Hack A Data Center
May 2010

SECURITYWEEK

Recent Bank Cyber Attacks Originated From Hacked Data Centers, Not Large Botnet *October, 2012*

COMPUTERWORLD

Hackers exploit SCADA holes to take full control of critical infrastructure *January, 2014*

NETWORKWORLD

Hacks to turn your wireless IP surveillance cameras against you *April, 2013*

GIZMODO

A Creepy Website Is Streaming From 73,000 Private Security Cameras *November, 2014*

WIRED

Popular Surveillance Cameras Open to Hackers, Researchers Say *May, 2012*

The Register®

DECT wireless eavesdropping made easy
December, 2013

HELP NET SECURITY

Is Your Cordless Phone Being Hacked?
March, 2014

NETWORKWORLD

DECT phones and POS terminals are vulnerable
January, 2009

InformationWeek DARKReading

Smart Meter Hack Shuts Off The Lights
September, 2014

KrebsonSecurity
In-depth security news and investigation

Target Hackers Broke in Via HVAC Company
February 2014

black hat®

Energy fraud and Orchestrated blackouts: Issues with wireless metering *July 214*

WIRED

This Hacked Kids' Toy Opens Garage Doors in Seconds *June, 2015*

engadget

This $30 device defeats almost any keyless car or garage door *April 2015*

MOTHERBOARD

This Kids' Toy Can Hack Garage Doors in Seconds *June 2015*

ZDNet

Tesla electric cars vulnerable to remote unlocking hack, researchers say *April, 2014*

WIRED

Hackers Remotely Kill a Jeep on the Highway—With Me in It. *July, 2015*

The Washington Post

‘Car hacking’ just got real: In experiment, hackers disable SUV on busy highway *July, 2015*

CSO

Rogue cell towers discovered in Washington, D.C
April, 2014

Forbes

Rogue Cell Towers Could Be Intercepting Your Call
September, 2014

BLACK BAG

Rogue "Interceptor" Cell Phone Towers Discovered Near U.S. Army Bases *September 2014*

WHAT COULD GO WRONG - PRIVACY

IoT Enabling Big Brother

- Impact insurance premiums
- Allow for discrimination

- Allow for off hours monitoring
- Track productivity

Bastille

Security for the Internet of Things